08-17-01

A

Please type a plus sign (+) inside this box → [+]

PTO/SB/05 (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	028420-0013CON
First Inventor	P. C. Kocher
Title	Cryptographic Computation Using Masking to Prevent ...
Express Mail Label No.	EL 728 498 770 US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: ~~Assistant~~ Commissioner for Patents, Box Patent Application, Washington, D.C. 20231

1. [✓] Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original, and a duplicate for fee processing)*
2. [ ] Applicant claims small entity status. See 37 CFR 1.27.
3. [✓] Specification *[Total Pages* 34 *]* *(preferred arrangement set forth below)*
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. [✓] Drawing(s) *(35 U.S.C. 113)* *[Total* 2 *]*
5. Oath or Declaration *[Total Pages* 2 *]*
   - a. [ ] Newly executed (original or copy)
   - b. [✓] Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional with Box 18 completed)*
     - i. [ ] DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. [ ] Application Data Sheet. See 37 CFR 1.76
7. [ ] CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   - a. [ ] Computer Readable Form (CRF)
   - b. Specification Sequence Listing on:
     - i. [ ] CD-ROM or CD-R (2 copies); or
     - ii. [ ] paper
   - c. [ ] Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. [ ] Assignment Papers (cover sheet & document(s))
10. [ ] 37 CFR 3.73(b) Statement *(when there is an assignee)* [✓] Power of Attorney (copy)
11. [ ] English Translation Document *(if applicable)*
12. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
13. [✓] Preliminary Amendment
14. [✓] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. [ ] Request and Certification under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. [✓] Other: Certificate of Mailing

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:*

[✓] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No.: 09/324,798

Prior application information: Examiner J. Darrow Group / Art Unit 2132

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

[ ] *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* or [X] *Correspondence address below*

Name	Joseph Yang, Ph.D.				
	Skadden, Arps, Slate, Meagher & Flom LLP				
Address	525 University Avenue				
City	Palo Alto	State	California	Zip Code	94301
Country	U.S.A.	Telephone	(650) 470-4500	Fax	(650) 470-4570

Name (Print/Type)	Joseph Yang, Ph.D.	Registration No. (Attorney/Agent)	41,387
Signature		Date	August 15, 2001

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

UTILITY PATENT APPLICATION TRANSMITTAL Page 2	Attorney Docket No.:	028420-0013CON
	First Inventor:	P. C. Kocher et al.
	Title:	Cryptographic Computation Using Masking to Prevent Differential Power Analysis and Other Attacks
	Express Mail Label No.:	EL 728 498 770 US

This is a Continuation Application under 37 C.F.R. § 1.53(b) of pending Application Serial No. 09/324,798 filed on June 3, 1999 (which, in turn, claims the benefit of Serial No. 60/087,826 filed June 3, 1998), for DES and Other Cryptographic Processes with Leak Minimization for Smartcards and Other Cryptosystems, by the following named inventors:

a. Full Name Paul C. Kocher
Citizenship United States of America
Residence San Francisco, California
Address 143 Fillmore Street, San Francisco, California 94117

b. Full Name Joshua M. Jaffe
Citizenship United States of America
Residence San Francisco, California
Address 200 Upper Terrace, Apt. 4, San Francisco, California 94117

c. Full Name Benjamin C. Jun
Citizenship United States of America
Residence Palo Alto, California
Address 1081-B Tanlan Drive, Palo Alto, California 94303

1. Enclosed is a copy of prior Application Serial No. 09/324,798 filed on June 3, 1999, including copies of the specification, claims, abstract and the executed oath or declaration as originally filed. Enclosed is a copy of the formal drawings submitted on March 28, 2001 in prior Application Serial No. 09/324,798 filed on June 3, 1999.

2. The filing fee is calculated below:

Basic Application Fee				$	710.00
Total Claims	10	Minus 20 = 0	x $18 =	$	0.00
Independent Claims	3	Minus 3 = 0	x $80 =	$	0.00
Total Application Fee Due				$	710.00

3. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 19-2385. A duplicate of this paper is enclosed.

UTILITY PATENT APPLICATION TRANSMITTAL Page 3	Attorney Docket No.:	028420-0013CON
	First Inventor:	P. C. Kocher et al.
	Title:	Cryptographic Computation Using Masking to Prevent Differential Power Analysis and Other Attacks
	Express Mail Label No.:	EL 728 498 770 US

4. A check in the amount of $710.00 is enclosed.

5. Cancel in this application original claims 1-40 of the prior application before calculating the filing fee.

6. The prior application is assigned of record to Cryptography Research, Inc., 870 Market Street, Suite 1088, San Francisco, California 94102 (assignment recorded June 3, 1999 at Reel 010010, Frame 0626).

7. A preliminary amendment is enclosed.

8. The power of attorney in the prior application is to:

Ronald S. Laurie, Reg. No. 25,431
Joseph Yang, Ph.D., Reg. No. 41,387
Frederick Hadidi, Reg. No. 37,342
Thomas Raleigh Lane, Reg. No. 42,781

a. A copy of the power in the prior application is enclosed.

b. Recognize as Associate Attorney:

Frederick D. Kim, Ph.D., Reg. No. 38,513
Stacey J. Farmer, Ph.D., Reg. No. 42,526
Robert B. Beyers, Ph.D., Reg. No. 46,552
Constance F. Ramos, Ph.D., Reg. No. 47,883
Gene I. Su, Reg. No. 45,140
Daniel J. Lin, Reg. No. 47,750

c. Address all future communications to:

Joseph Yang, Ph.D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, California 94301

Date: August 15, 2001

By: _____
Joseph Yang, Ph.D.
Registration No. 41,387

Address of signator:

Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, California 94301
Telephone: (650) 470-4500
Facsimile: (650) 470-4570

Inventor(s)
Assignee of complete interest
X Attorney or agent of record
filed under 37 C.F.R. § 1.34(a)

PTO/SB/17 (08-00)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to r espond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT $710.00

Complete if Known	
Application Number	Unknown
Filing Date	August 15, 2001
First Named Inventor	P. C. Kocher
Examiner Name	J. Darrow
Group / Art Unit	2132
Attorney Docket No.	028420-0013CON

METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number: 19-2385

Deposit Account Name: Skadden, Arps et al.

☒ Charge Any Additional Fee Required Under 37 CFR §§ 1.16 and 1.17

☐ Applicant claims small entity status. See 37 CFR § 1.27

2. ☒ Payment Enclosed:

☒ Check ☐ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	710.00
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) $710.00

2. EXTRA CLAIM FEES

	Extra Claims			Fee from below	Fee Paid
Total Claims	10	-20** =	0	X =	0.00
Independent Claims	3	-3** =	0	X =	0.00
Multiple Dependent				=	

**or number previously paid, if greater; For Reissues, see below

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) $0.00

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non - English specification	
147	2,520	147	2,520	For filing a request for *ex parte* reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Statement	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

Reduced by Basic Filing Fee Paid . SUBTOTAL (3)

SUBMITTED BY

Complete *(if applicable)*

Name (Print/Type)	Joseph Yang, Ph.D.	Registration No. (Attorney/Agent)	41,387	Telephone	(650) 470-4500
Signature				Date	August 15, 2001

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10) Applicant(s): **P. C. Kocher et al.**	Docket No. **028420-0013CON**

Serial No.	Filing Date	Examiner	Group Art Unit
Unknown	**August 15, 2001**	**J. Darrow**	**2132**

Invention:

Cryptographic Computation Using Masking to Prevent Differential Power Analysis and Other Attacks

I hereby certify that this **Utility Patent Application Transmittal and all enclosures**
(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: ~~The Assistant~~ Commissioner for Patents, Washington, D.C. 20231 on

August 15, 2001
(Date)

Jan Steele
(Typed or Printed Name of Person Mailing Correspondence)

Jan Steele
(Signature of Person Mailing Correspondence)

EL 728 498 770 US
("Express Mail" Mailing Label Number)

PTO/SB/29 (08-00)

Note: Each paper must have its own certificate of mailing.

Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, California 94301
United States of America
Telephone: (650) 470-4500
Facsimile: (650) 470-4570